SUZANNE M. DUGAN
SPECIAL COUNSEL
202.408.4600
sdugan@cohenmilstein.com
V-CARD

FIDUCIARY FOCUS

3x

"Attempts to breach the system are increasing at a rapid rate. We might have had two or three attempts to redirect electronic deposits two years ago, then it jumped 30-fold last year, and we are on track to triple that this year."

AN INTERVIEW ON CYBERSECURITY WITH BRIAN BARTOW OF THE CALIFORNIA STATE TEACHERS' RETIREMENT SYSTEM

Spend some time with Brian Bartow and you'll soon learn that worrying about cybersecurity is what keeps him up at night. If you're having trouble getting your arms around cybersecurity and its implications for your pension system, Brian's expertise and cool demeanor in this area are just what you need to help you focus on this critical risk. As the General Counsel and Chief Compliance Officer at CalSTRS, Brian is responsible for enterprise information management and information security. He has even taught a law school class on the topic. Brian sat down for an interview to share his knowledge and insights about the fiduciary obligations arising out of the risks associated with cybersecurity.

Suzanne Dugan, Cohen Milstein: How serious is the cybersecurity threat to pension systems?

Brian Bartow, CalSTRS: Except for funding, it is the number one risk we face. When you assess risk, the analysis is typically two dimensional—that is, we look at the severity of the risk and the likelihood of its occurrence. With cybersecurity risk, there is an added third dimension. In addition to severity and likelihood, we assess the velocity of the risk. If a breach happens, it's going to happen immediately, whether the breach affects one record or brings down the whole system. This is not theoretical.

What got my attention was the severity and reality of the risk. The whole enterprise is at risk. I started talking about this issue about five years ago and although the word does seem to be getting out, I'm still amazed at the lack of engagement on this issue by those who still consider cyber and information security as to be IT issues. We should be concerned at the lack of comprehension of the inevitability and the potential dimensions of this risk.

Dugan: Is the risk increasing?

Bartow: Absolutely. Attempts to breach the system are increasing at a rapid rate. We might have had two or three attempts to redirect electronic deposits two years ago, then it jumped 30-fold last year, and we are on track to triple that this year. There is so much information now available on the dark web, from new breaches and from internet vapor trails, malefactors are able to capitalize on this and create synthetic identities from which they can launch targeted, coordinated and sophisticated attacks. This uptick was fueled by the breaches that released personal information such as the Anthem and Equifax breaches where information like social security numbers, age, workplace, and health information was stolen and now can be cross-referenced with other publicly available information like name, salary and workplace. Malefactors are infinitely resourceful and very motivated. Our team constantly monitors information sources through data analytics so that we can identify deviations in the use and direction of data, levels of usage and patterns of access, from which we develop early indicators and investigate and respond immediately.

Dugan: What steps should a pension plan be taking?

BRIAN BARTOW

Bartow: First and foremost, the cybersecurity threat must be characterized as a fiduciary responsibility and identified as a risk so that it is brought to the board's attention. That step is critical to every other action that follows. The board must then come up with a budgetary device recognizing that this threat constitutes an expenditure line item. Addressing the critical risk of cybersecurity requires a commitment of resources. There's no way around that.

The next step is to perform an audit, whether internal or external, looking at the existing internal controls in the area of information security and reporting on cybersecurity risk. This audit should lay the framework for how to address the risks and mature the security posture. Cyber risks can fall into various categories, which may be isolated or run across the organization, such as operational, financial, and reputational. Information and cyber security threats and risks may come from third parties, such as employers, vendors or contractors. These risks should be addressed and mitigated as possible through contractual terms or insurance. A cyber plan can begin to be developed from this assessment. Systems can then be developed and implemented to address the risks. Other ways to manage the risks might involve purchasing cybersecurity insurance—the cost of which has come down of late—and including contractual provisions assigning risk and responsibility or providing for indemnification.

> *"First and foremost, the cybersecurity threat must be characterized as a fiduciary responsibility and identified as a risk so that it is brought to the board's attention."*

I meet with my direct reports involved in managing these risks every two weeks for 2 ½ hours. Our plan requires that roles are clearly defined so that, if a breach occurs, there is no hesitation by those who must take action to manage and contain the intrusion into our data. Those with responsibility are authorized to break from their usual duties and their usual reporting requirements to empower them to attend to and execute the plan. Considering the immediacy of impact on the system from a breach and the broad potential for harm, this kind of attention is critical and should become "muscle memory" for the organization.

Dugan: Is there any guidance or advice regarding best practices?

Bartow: A number of organizations have begun to develop some reports that suggest ways to manage these risks. Among those are the AICPA, National Association of Corporate Directors, the SEC and the Center for Internet Security. There are others but we must absolutely appreciate that these risks are ongoing and constantly evolving so that eternal vigilance is essential. The best deterrence is knowing your data and who is touching it, as different kinds of data create different kinds of risks. Data Loss Prevention is an important focus of any program. Collecting this information and reviewing it regularly are essential components to planning and implementation. You really have to drill down and understand these variations and respond quickly and appropriately.

Dugan: CalSTRS is a big fund with lots of resources. What about smaller funds with less capacity and fewer resources?

Bartow: The risks are the same for funds of any size. The appeal of the data to bad guys is the same regardless of the number of records or amount of money under management. A breach can be devastating. It means that the steps outlined here, from getting the board's attention to prioritizing these issues to assessing these risks to developing and implementing plans, are the same. It may be that resources will affect the extent of a response but should not be a barrier to an organization identifying the issue as a priority and assessing the attendant risks. Considering the operational, financial, and reputational risks, those steps are critical to fulfilling a board's fiduciary duty.

Dugan: Brian, thank you for your guidance in this area. ■